



# CVE-2023-4623

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2023-4623   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | security@google.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2023-09-06 14:15:00 UTC   |
| <b>Updated</b>         | 2023-10-29 02:40:00 UTC   |
| <b>Description</b>     | A use-after-free vulnerability in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component can be exploi |

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                      | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a> | 2.6.12  | rc1    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |

## References

| Reference  | Source  | Link                             | Tags                |
|--|---------|----------------------------------|---------------------|
| [SECURITY] [DLA 3623-1] linux-5.10 security update       | MISC    | <a href="#">lists.debian.org</a> |                     |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC    | <a href="#">git.kernel.org</a>   |                     |
| kernel.dance/b3d26c5702c7d6c45456326e56d2ccf3f103e60f    | MISC    | <a href="#">kernel.dance</a>     |                     |
| CVE Program record                                       | CVE.ORG | <a href="#">www.cve.org</a>      | canonical           |
| NVD vulnerability detail                                 | NVD     | <a href="#">nvd.nist.gov</a>     | canonical, analysis |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[161220](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-13039)

|  |
|--|
| <a href="#">161237</a> Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-13043) |
| <a href="#">161339</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2024-12149)                        |
| <a href="#">161390</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2024-12187)                        |
| <a href="#">161402</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2024-0897)                         |
| <a href="#">161404</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2024-0461)                         |
| <a href="#">199803</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6415-1)            |
| <a href="#">199841</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6444-1)                  |
| <a href="#">199842</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6440-1)                  |
| <a href="#">199843</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6439-1)                  |
| <a href="#">199844</a> Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6445-1)     |
| <a href="#">199845</a> Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6442-1)      |
| <a href="#">199846</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6441-1)                  |
| <a href="#">199848</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6446-1)                  |
| <a href="#">199849</a> Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-6440-2)          |
| <a href="#">199854</a> Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-6441-2)            |
| <a href="#">199855</a> Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6439-2)            |
| <a href="#">199858</a> Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6445-2)     |
| <a href="#">199859</a> Ubuntu Security Notification for Linux kernel (StarFive) Vulnerabilities (USN-6444-2)       |
| <a href="#">199861</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6446-2)                  |
| <a href="#">199864</a> Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-6440-3)            |
| <a href="#">199868</a> Ubuntu Security Notification for Linux kernel (Oracle) Vulnerabilities (USN-6446-3)         |
| <a href="#">199872</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6441-3)                  |
| <a href="#">199874</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6460-1)                  |
| <a href="#">199883</a> Ubuntu Security Notification for Linux kernel (NVIDIA) Vulnerabilities (USN-6466-1)         |
| <a href="#">242727</a> Red Hat Update for kpatch-patch (RHSA-2024:0340)  |
| <a href="#">242728</a> Red Hat Update for kpatch-patch (RHSA-2024:0378)  |
| <a href="#">242734</a> Red Hat Update for kpatch-patch (RHSA-2024:0381)  |
| <a href="#">242738</a> Red Hat Update for kpatch-patch (RHSA-2024:0386)  |
| <a href="#">242759</a> Red Hat Update for kernel (RHSA-2024:0432)  |

|  |
|--|
| <a href="#">242769</a> Red Hat Update for kpatch-patch (RHSA-2024:0554)                              |
| <a href="#">242785</a> Red Hat Update for kpatch-patch (RHSA-2024:0593)                              |
| <a href="#">242789</a> Red Hat Update for kernel (RHSA-2024:0575)                                    |
| <a href="#">242830</a> Red Hat Update for kernel-rt (RHSA-2024:0563)                                 |
| <a href="#">242831</a> Red Hat Update for kernel (RHSA-2024:0562)                                    |
| <a href="#">242839</a> Red Hat Update for kernel (RHSA-2024:0461)                                    |
| <a href="#">242845</a> Red Hat Update for kernel (RHSA-2024:0448)                                    |
| <a href="#">242846</a> Red Hat Update for kernel-rt (RHSA-2024:0439)                                 |
| <a href="#">242847</a> Red Hat Update for kernel-rt (RHSA-2024:0431)                                 |
| <a href="#">242855</a> Red Hat Update for kernel (RHSA-2024:0412)                                    |
| <a href="#">242938</a> Red Hat Update for kpatch-patch (RHSA-2024:0876)                              |
| <a href="#">242939</a> Red Hat Update for kernel (RHSA-2024:0897)                                    |
| <a href="#">242983</a> Red Hat Update for kernel-rt (RHSA-2024:0881)                                 |
| <a href="#">243055</a> Red Hat Update for kernel (RHSA-2024:1268)                                    |
| <a href="#">243057</a> Red Hat Update for kpatch-patch (RHSA-2024:1278)                              |
| <a href="#">243058</a> Red Hat Update for kernel-rt (RHSA-2024:1269)                                 |
| <a href="#">356357</a> Amazon Linux Security Advisory for kernel : ALAS-2023-1838                    |
| <a href="#">356371</a> Amazon Linux Security Advisory for kernel : ALAS2023-2023-356                 |
| <a href="#">356409</a> Amazon Linux Security Advisory for kernel : ALAS2-2023-2264                   |
| <a href="#">356567</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-027         |
| <a href="#">356571</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-155 |
| <a href="#">356572</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-040         |
| <a href="#">356577</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-150 |
| <a href="#">356584</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-152 |
| <a href="#">356588</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-154 |
| <a href="#">356595</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-153 |
| <a href="#">356599</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-151 |
| <a href="#">356606</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-053          |

|   |
|---|
| <a href="#">356611</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-149                                      |
| <a href="#">356919</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-026                                   |
| <a href="#">356923</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-024                                   |
| <a href="#">356924</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-025                                   |
| <a href="#">379043</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0136)  |
| <a href="#">379435</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2024:0012)  |
| <a href="#">6000265</a> Debian Security Update for linux-5.10 (DLA 3623-1)  |
| <a href="#">6000429</a> Debian Security Update for linux (DLA 3710-1)   |
| <a href="#">6140413</a> AWS Bottlerocket Security Update for kernel (GHSA-5956-78jx-7225)   |
| <a href="#">673406</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3182)  |
| <a href="#">673563</a> EulerOS Security Update for kernel (EulerOS-SA-2024-1144)  |
| <a href="#">673595</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3247)  |
| <a href="#">673644</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3336)  |
| <a href="#">673692</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3275)  |
| <a href="#">673848</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3217)  |
| <a href="#">673995</a> EulerOS Security Update for kernel (EulerOS-SA-2024-1275)  |
| <a href="#">674042</a> EulerOS Security Update for kernel (EulerOS-SA-2023-3304)  |
| <a href="#">755059</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4035-1)                                   |
| <a href="#">755060</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4031-1)                                   |
| <a href="#">755061</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4030-1)                                   |
| <a href="#">755063</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4032-1)                                   |
| <a href="#">755082</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4058-1)                                   |
| <a href="#">755083</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4057-1)                                   |
| <a href="#">755085</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4072-1)                                   |
| <a href="#">755086</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4071-1)                                   |
| <a href="#">755096</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4093-1)                                   |
| <a href="#">755107</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4095-1)                                   |
| <a href="#">755135</a> SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 5 for SLE 15 SP4) (SUSE-SU-2023:4166-1)  |
| <a href="#">755136</a> SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 11 for SLE 15 SP4) (SUSE-SU-2023:4165-1) |

[755136](#) SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 11 for SLE 15 SP4) (SUSE-SU-2023:4165-1)

[755137](#) SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 13 for SLE 15 SP4) (SUSE-SU-2023:4164-1)

[755140](#) SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 1 for SLE 15 SP5) (SUSE-SU-2023:4175-1)

[755148](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 18 for SLE 15 SP4) (SUSE-SU-2023:4328-1)

[755154](#) SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 3 for SLE 15 SP4) (SUSE-SU-2023:4201-1)

[755168](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 33 for SLE 15 SP3) (SUSE-SU-2023:4219-1)

[755178](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 36 for SLE 15 SP3) (SUSE-SU-2023:4261-1)

[755179](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 35 for SLE 15 SP3) (SUSE-SU-2023:4260-1)

[755180](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 33 for SLE 15 SP2) (SUSE-SU-2023:4245-1)

[755181](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 35 for SLE 15 SP1) (SUSE-SU-2023:4244-1)

[755182](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 40 for SLE 15 SP2) (SUSE-SU-2023:4243-1)

[755184](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15 SP3) (SUSE-SU-2023:4239-1)

[755186](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 4 for SLE 15 SP4) (SUSE-SU-2023:4267-1)

[755192](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 7 for SLE 15 SP4) (SUSE-SU-2023:4285-1)

[755193](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 44 for SLE 15 SP1) (SUSE-SU-2023:4280-1)

[755194](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 34 for SLE 15 SP2) (SUSE-SU-2023:4279-1)

[755195](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 15 SP1) (SUSE-SU-2023:4278-1)

[755196](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 16 for SLE 15 SP4) (SUSE-SU-2023:4301-1)

[755197](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 39 for SLE 12 SP5) (SUSE-SU-2023:4300-1)

[755210](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 8 for SLE 15 SP4) (SUSE-SU-2023:4308-1)

[755212](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2023:4326-1)

[755213](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 3 for SLE 15 SP5) (SUSE-SU-2023:4325-1)

[755214](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 15 for SLE 15 SP4) (SUSE-SU-2023:4322-1)

[755215](#) SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 12 SP5) (SUSE-SU-2023:4321-1)

[755229](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4072-2)

[755565](#) SUSE Security Update for the linux kernel (SUSE-SU-2023:4347-1)

[907559](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (31697-1)

[941584](#) AlmaLinux Security Update for kernel (ALSA-2024:0897)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**